UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,004	08/17/2001	Nang Kon Kwan	06502.0336	2756

7590 11/23/2004

Finnegan, Henderson, Farabow,
Garrett & Dunner, L.L.P.
1300 I Street, N.W.
Washington, DC 20005-3315

EXAMINER	
CHAI, LONGBIT	

ART UNIT	PAPER NUMBER
2131	3

DATE MAILED: 11/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/931,004	KWAN, NANG KON	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 October 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 October 2003* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. No claim for priority has been made in this application.

2. The effective filing date for the subject matter defined in the pending claims in this application is 08/17/2001.

Specification

3. The disclosure is objected to because of the following informalities:

4. The last sentence of 23rd Paragraph is incomplete which is ended with "with the". See 37 CFR 1.71. Appropriate correction is required.

Drawings

1. Figure 2 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.121(d)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1 – 6, 9 – 10, 12, 14 – 24, 27 – 28, 30 and 32 – 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over AAP (Applicant Admitted Prior-Art: Patent Number: 2003/0035548 A1), hereinafter referred to as AAP, in view of Cooper (Patent Number: 2002/0029350 A1), hereinafter referred to as Cooper.

As per claim 1, 19, 15 and 33, AAP teaches a method in a data processing system for requesting a digital certificate from a certificate authority (AAP: see for example, Figure 2 and Paragraph [0034] & [0035]).

AAP does not teach archiving an encryption key outside of the certificate authority.

Cooper teaches archiving an encryption key outside of the certificate authority (Cooper: see for example, Paragraph [0204] Line 7, Figure 3 Element 240, 260 & 270, and Paragraph [0005], [0052]: Cooper teaches (a) the encryption keys are stored and archived by a neural third party, and (b) the consultation module comprises an archiving capability provided by an archive module where a list of consultants can be selected under the choice of the client (Cooper: see for example, Paragraph [0146] and Claim 7

– 6th & 7th Paragraphs). Therefore, the consultant database module as taught by Cooper in Figure 3 Element 260 which is directly interfaced with the client is qualified as the registration module as taught by AAP.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Cooper within the system of AAP because Cooper teaches a technique to issue a digital certificate through a virtual private network (VPN) which allows the client to exchange information with consultant database module under the client choice to provide an enhanced secure user-friendly environment (Cooer: see for example, Paragraph [0003], [0009] and Claim 7 – 6th & 7th Paragraphs).

Therefore, AAP as modified teaches a method in a data processing system for requesting a digital certificate from a certificate authority and archiving an encryption key outside of the certificate authority, comprising:

receiving a request from a user for a digital certificate (See addressed above);

receiving an indication of proof of archival of the user's encryption key associated with the request, wherein the user's encryption key is archived under control of an entity other than the certificate authority (See addressed above – Besides, an indication message is commonly used between two software entities in the field).

As per claim 10, 16 and 28, AAP teaches a method in a data processing system for requesting a digital certificate from a certificate authority (AAP: see for example, Figure 2 and Paragraph [0034] & [0035]).

AAP does not teach archiving an encryption key outside of the certificate authority.

Cooper teaches archiving an encryption key outside of the certificate authority (Cooper: see for example, Paragraph [0204] Line 7, Figure 3 Element 240, 260 & 270, and Paragraph [0005], [0052]: Cooper teaches (a) the encryption keys are stored and archived by a neural third party, and (b) the consultation module comprises an archiving capability provided by an archive module where a list of consultants can be selected under the choice of the client (Cooper: see for example, Paragraph [0146] and Claim 7 – 6th & 7th Paragraphs). Therefore, the consultant database module as taught by Cooper in Figure 3 Element 260 which is directly interfaced with the client is qualified as the registration module as taught by AAP

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Cooper within the system of AAP because Cooper teaches a technique to issue a digital certificate through a virtual private network (VPN) which allows the client to exchange information with consultant database module under the client choice to provide an enhanced secure user-friendly environment (Cooer: see for example, Paragraph [0003], [0009] and Claim 7 – 6th & 7th Paragraphs).

Therefore, AAP as modified teaches a method in a data processing system for requesting a digital certificate from a certificate authority and archiving an encryption key outside of the certificate authority, comprising:

sending a request for a digital certificate (AAP: see for example, Figure 2 and Paragraph [0034] & [0035]);

the request having an indication of proof of archival of an encryption key for the user (Cooer: see for example, Paragraph [0052], [0146], and [0204]: Cooper teaches the encryption keys can be generated by the archive module in the consultation database module where the consultant is selected by the client – See claim 1 addressed above and furthermore, an indication message is commonly used between two software entities in the field); and

receiving a digital certificate in response to the request (AAP: see for example, Figure 2 and Paragraph [0034] & [0035]).

As per claim 18, AAP teaches AAP teaches a data processing system for requesting a digital certificate from a certificate authority (AAP: see for example, Figure 2 and Paragraph [0034] & [0035]).

AAP does not teach archiving an encryption key outside of the certificate authority.

Cooper teaches archiving an encryption key outside of the certificate authority (Cooper: see for example, Paragraph [0204] Line 7, Figure 3 Element 240, 260 & 270, and Paragraph [0005], [0052]: Cooper teaches (a) the encryption keys are stored and archived by a neural third party, and (b) the consultation module comprises an archiving capability provided by an archive module where a list of consultants can be selected under the choice of the client (Cooper: see for example, Paragraph [0146] and Claim 7

– 6th & 7th Paragraphs). Therefore, the consultant database module as taught by Cooper in Figure 3 Element 260 which is directly interfaced with the client is qualified as the registration module as taught by AAP.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Cooper within the system of AAP because Cooper teaches a technique to issue a digital certificate through a virtual private network (VPN) which allows the client to exchange information with consultant database module under the client choice to provide an enhanced secure user-friendly environment (Cooer: see for example, Paragraph [0003], [0009] and Claim 7 – 6th & 7th Paragraphs).

Therefore, AAP as modified teaches a data processing system for requesting a digital certificate from a certificate authority and archiving an encryption key under control of an entity other than the certificate authority, comprising:

a data recovery manager configured to receive the user's encryption key (AAP: see for example, Figure 2 and Paragraph [0034] & [0035]), and send the user's encryption key to a database controlled by an entity other than the certificate authority for archiving, create an indication of proof archival and send the indication of proof of archival (Cooper: see for example, Paragraph [0204], [0146] and [0149]: The archive module as taught by Cooper is qualified as the data recovery manager which can store and archive the encryption keys (Cooper: see for example, Paragraph [0204]). This archive module is part of the consultation database module which is controlled by the client by selecting the desired consultant (Cooper: see for example, Paragraph [0146] &

[0149] and Claim 7 6th & 7th Paragraphs). Thereby, the data recovery manager is controlled by an entity other than the certificate authority for archiving.

a registration manager configured to receive a digital certificate request including a user's encryption key, send the user's encryption key, and in response receive an indication of proof of archival (AAP: see for example, Figure 2 Paragraph [0034] & [0035]) and (Cooper: see for example, Figure 3 Element 260, Paragraph [0146] and Claim 7 – 6th & 7th Paragraphs: The consultant database module as taught by Cooper in Figure 3 Element 260 which is directly interfaced with the client is qualified as the registration module as taught by AAP because the consultation module comprises an archiving capability provided by an archive module where a list of consultants can be selected under the choice of the client (Cooper: see for example, Paragraph [0146] and Claim 7 – 6th & 7th Paragraphs).

a certificate authority configured to issue a digital certificate when it is determined that an indication proof of archival was received (Cooper: see for example, Paragraph [0146]: Cooper teaches the encryption key can also be generated by the archive module which is independent to the CA as addressed above. Thereby a certificate authority should confirm an indication proof of archival was received before issuing a digital certificate).

a database, under control of an entity other than the certificate authority, configured to receive and archive the user's encryption key (See addressed above).

As per claim 2 and 20, AAP as modified teaches the claimed invention as described above (see claim 1 and 19 respectively). AAP as modified further teaches the step of sending a digital certificate associated with the user in response to the received request and indication of proof of archival (Cooper: see for example, Figure 3 and Paragraph [0050]).

As per claim 3 and 21, AAP as modified teaches the claimed invention as described above (see claim 1 and 19 respectively). AAP as modified further teaches the step of receiving the user's encryption key (AAP: see for example, Figure 2 and Paragraph [0034] & [0035]).

As per claim 4 and 22, AAP as modified teaches the claimed invention as described above (see claim 3 and 21 respectively). AAP as modified further teaches the encryption key is encrypted during transmission, and wherein the method further comprises the step of decrypting the encrypted encryption key (AAP: see for example, Figure 2 and Paragraph [0035] Line 6).

As per claim 5 and 23, AAP as modified teaches the claimed invention as described above (see claim 3 and 21 respectively). AAP as modified further teaches the encryption key is the user's private key (AAP: see for example, Figure 2 and Paragraph [0035] Line 5 – 6) & (Cooper: see for example, Figure 3 and Paragraph [0051] and [0052]).

As per claim 6 and 24, AAP as modified teaches the claimed invention as described above (see claim 4 and 22 respectively). AAP as modified further teaches a data recovery manager that receives and manages archiving of the encryption key, and wherein the encryption key is encrypted during transmission using the data recovery manager's public transport key (Cooper: see for example, Figure 3 and Paragraph [0204] – [0206]) and (AAP: see for example, Paragraph [0035]).

As per claim 9, 14, 27 and 32, AAP as modified teaches the claimed invention as described above (see claim 1, 13, 19 and 31 respectively). AAP as modified teaches the user's encryption key is archived under control of the user ((Cooper: see for example, Paragraph [0204] Line 7, Figure 3 Element 240, 260 & 270, and Paragraph [0005], [0052]: Cooper teaches (a) the encryption keys are stored and archived by a neural third party, and (b) the consultation module comprises an archiving capability provided by an archive module where a list of consultants can be selected under the choice of the client (Cooper: see for example, Paragraph [0146] and Claim 7 – 6th & 7th Paragraphs). Therefore, the consultant database module as taught by Cooper in Figure 3 Element 260 which is directly interfaced with the client is qualified as the registration module as taught by AAP

As per claim 12, 17 and 30, claims 12, 17 and 30 do not further teach over claim 1. Therefore, see rationale addressed above in rejecting claim 1.

6. Claims 7 – 8, 11, 13, 25 – 26, 29 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over AAP (Applicant Admitted Prior-Art: Patent Number: 2003/0035548 A1), hereinafter referred to as AAP, in view of Cooper (Patent Number: 2002/0029350 A1), hereinafter referred to as Cooper, an in view of Okuruma (Patent Number: US 6553493 B1) Okuruma.

As per claim 7, 11, 13, 25, 29 and 31, AAP as modified teaches the claimed invention as described above (see claim 1, 10, 12, 19, 28 and 30 respectively). AAP as modified teaches receiving an indication of proof of archival of the user's encryption key associated with the request, wherein the user's encryption key is archived under control of an entity other than the certificate authority (Cooper: see for example, Paragraph [0204] Line 7, Figure 3 Element 240, 260 & 270, and Paragraph [0005], [0052]: Cooper teaches (a) the encryption keys are stored and archived by a neural third party, and (b) the consultation module comprises an archiving capability provided by an archive module where a list of consultants can be selected under the choice of the client (Cooper: see for example, Paragraph [0146] and Claim 7 – 6th & 7th Paragraphs: Therefore, the consultant database module as taught by Cooper in Figure 3 Element 260 which is directly interfaced with the client is qualified as the registration module as taught by AAP) – Besides, an indication message is commonly used between two software entities in the field).

However, AAP as modified does not teach the indication of proof of archival is digitally signed.

Okumura teaches the indication of proof of archival is digitally signed (Okuruma: see for example, Column 4 Line 19 – 32: OKuruma teaches using the private key to "digitally sign" a digital message (such as indication message) which is often referred to as "proof of origin").

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Okumura within the system of AAP as modified because Okumura teaches an enhanced security technique of digitally signing a message using a private key before sending to the receiver and using the public key for validation on the reception of the message).

Therefore, AAP as modified teaches the indication of proof of archival is digitally signed, and wherein the method further comprises the step of verifying a digital signature on the indication of proof of archival (Okuruma: see for example, Column 4 Line 19 – 32).

As per claim 8 and 26, AAP as modified teaches the claimed invention as described above (see claim 7 and 25 respectively). AAP as modified teaches the data processing system includes a data recovery manager that receives and manages archiving of the encryption key, and wherein the indication of proof of archival is digitally signed by the data recovery manager (See the same rationale addressed as above in

rejecting claim 18 – The archive module as taught by Cooper is qualified as the Data Recovery Manager).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 703-305-0710. The examiner can normally be reached on Monday-Friday 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100